DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)

	a. PRIME CONTRACT NUMBER		X	a. ORIGINAL (Complete date in all cases) — Date (YYMMDD): 20021024
	b. SUBCONTRACT NUMBER			b. REVISED (Supersedes all previous specs) — Revision No. — Date (YYMMDD):
X	c. SOLICITATION OR OTHER NO.: N66001-03-R-0009	Due Date (YYMMDD):		c. FINAL (Complete Item 5 in all cases) — Date (YYMMDD):

3. THIS SPECIFICATION IS: (X and complete as applicable)

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO. If Yes, complete the following:

Classified material received or generated under (Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO. If Yes, complete the following:

In response to the contractor's request dated , retention of the identified classified material is authorized for the period of

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)
THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)

8. ACTUAL PERFORMANCE

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

PROVIDE TECHNICAL SERVICES TO UPDATE EXISTING NAVIGATION SYSTEM, HARDWARE AND SOFTWARE TECHNICAL MANUALS AND PROVIDE NEW SYSTEM HARDWARE AND SOFTWARE TECHNICAL MANUALS.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS	X	
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		
k. OTHER (Specify) SAP NO.: 1000000490					

SAP NO.: 1000000490 **CONTRACT NUMBER: N66001-03-R-0009**

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release to the Directorate for Freedom of Information and

☐ DIRECT ☒ THROUGH (Specify):

COMMANDING OFFICER, SPAWAR SYSTEMS CENTER CODE 2003, 53560 HULL STREET, SAN DIEGO CA 92152-5001

Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

CLASSIFICATION GUIDES:

NAVSTAR GLOBAL POSITIONING SYSTEM (GPS) SECURITY CLASSIFICATION GUIDE DTD 23 JULY 1984

ALL REQUESTS FOR INFORMATION SHOULD BE DIRECTED TO THE CONTRACTING OFFICER CODE 2211, TELEPHONE (619) 553-4462.

ALL CLASSIFIED INFORMATION MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 12958-CLASSIFIED NATIONAL SECURITY INFORMATION, OF 17 APRIL 1995. YOUR DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY REPRESENTATIVE (IS REP) SHOULD BE CONTACTED FOR ASSISTANCE.

COPIES OF ALL SUBCONTRACT DD FORM 254'S MUST BE PROVIDED TO THE DISTRIBUTION LISTED IN BLOCK 17.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed ☒ YES ☐ NO

SPECIFIC ON-SITE SECURITY REQUIREMENTS ARE ATTACHED.
FOR OFFICIAL USE ONLY (FOUO) INFORMATION IS ATTACHED.
INFORMATION TECHNOLOGY (IT) PERSONNEL SECURITY PROGRAM REQUIREMENTS IS ATTACHED.
TEMPEST REQUIREMENTS QUESTIONNAIRE WILL BE PROVIDED UPON CONTRACT AWARD.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) ☐ YES ☒ NO

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
PATTI.TALLEY@NAVY.MIL P. A. TALLEY	SECURITY'S CONTRACTING OFFICER'S REPRESENTATIVE (COR)	(619) 553-3195

d. ADDRESS (Include Zip Code)
COMMANDING OFFICER
SPAWAR SYSTEMS CENTER CODE 20351
53560 HULL ST.
SAN DIEGO, CA 92152-5001

e. SIGNATURE
20021024

17. REQUIRED DISTRIBUTION
☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER CODE 2211
☒ f. OTHERS AS NECESSARY CODES 20351, 2313

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS

Authority/Purpose:

The U.S. Government conducts trustworthiness investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified information technology (IT) resources and systems that process For Official Use Only (FOUO) and other controlled unclassified information.

The United States Office of Personnel Management (OPM), Investigations Service (IS), Federal Investigations Processing Center (FIPC) has been delegated authority to process all requests for U.S. Government trustworthiness investigations. Requirements for these investigations are outlined in paragraph C3.6.15 and Appendix 10 of DoD 5200.2-R, available at http://www.ntis.gov/. Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories listed below. The contractor shall include all of these requirements in any subcontracts involving IT support.

The Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the IT Position category to contractor personnel and inform the contractor of their determination. If it is decided the contractor shall make the assignment, the COR or TR must concur with the designation.

According to DoD 5200.28 (Security Requirements for Automated Information Systems), paragraph 4.10 which states "Access by foreign nationals to a U.S. Government-owned or U.S. Government-managed AIS may be authorized only by the DOD Component Head, and shall be consistent with the DOD, Department of State, and the Director of Central Intelligence policies." The Office of the Secretary of the Navy (SECNAV) approval is required for all non-U.S. citizens. All requests requiring SECNAV approval shall be submitted to the Space and Naval Warfare Systems Center (SSC San Diego), 53560 Hull Street, Code 20351, San Diego, CA 92152-5001.

Criteria For Designating Positions:

IT-I Position (High Risk)

- Responsibility or the development and administration of Government computer security programs, and also including direction and control of risk analysis an/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-I category to ensure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- Other positions as designated by SPAWARSYSCEN San Diego CA that involve relatively high risk for effecting grave damage or realizing significant personal gain.

Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years.

IT-II Position (Moderate Risk)

Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT-I category, includes but is not limited to:

- access to an/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

- accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by SPAWARSYSCEN San Diego CA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT-I positions. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check (NAC).

IT-III Position (Low Risk) -

- All other positions involving Federal IT activities. Incumbent in this position has non-privileged access to one or more DoD information systems/application or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated NAC.

Qualified Cleared Personnel Do NOT Require Trustworthiness Investigations:

If an employee is in a position that **does not** require a personnel security clearance, **do not** submit a request for clearance, simply submit the SF85P for trustworthiness determination. If an employee has already been granted a personnel security clearance at the appropriate level without a break in service for more than 24 months, and in the case of IT-I Position has had a completed Personnel Security Investigation (a Single Scope Background Investigation-SSBI) less than 5 years old, you do **not** need to submit an additional investigation for the trustworthiness determination.

Procedures for submitting U.S. Government Trustworthiness Investigations:

The contractor will ensure personnel designated IT-I, II, or III complete either the hard copy Standard Form (SF) 85P *or* the online—electronic (Electronic Personnel Security Questionnaire—EPSQ) version of the SF85P. Instructions on where to obtain and how to complete the SF85P are found below.

The investigative request package for the SF85P from the OPM web site (non-EPSQ) version consists of the following: 1) Completed and Validated Error-free SF85P; 2) OPM Fingerprint Card SF 87; 3) Security Officer's portion of the SF85P, and 4) signed Privacy Act release (to include a signed Medical release, when applicable). Note: Do not complete a separate OPM coversheet if using this SF85P form. The SF85P is available from OPM at http://www.opm.gov/forms/pdfimage/sf0085p.pdf with additional assistance at https://www.dss.mil.

When using the SF85P--EPSQ version, the submitted package shall include: 1) A hard copy of the SF85P, 2) all pertinent signed release forms, 3) OPM Fingerprint Card SF 87; 4) Employee's and Security Officer's validation certificates; and 5) an OPM coversheet signed and dated by the employee and FSO. The FSO is responsible for completing the OPM coversheet that is available for downloading with instructions at: http://www.opm.gov/extra/investigate/dodsf85.pdf. Note: For item "J" on this coversheet, use your company's Submitting Office Number (SON). If this is not available, contact OPM-FIPC Program Services Office (PSO) to apply for a SON by calling 724.794.5612. For item " L" insert "N030". Then for item "N" enter "DSS-IND".

The company shall review the SF85P for completeness and use SECNAVINST 5510.30A, Appendix G available at http://neds.nebt.daps.mil/551030.htm to determine if any adverse information is present. ***Only hard copy SF85Ps are acceptable by OPM-FIPC***. Additional guidance for requesting investigations from OPM is found at http://www.opm.gov/extra/investigate/IS-15.pdf. Completed SF85P packages will be mailed to: OPM-FIPC, P.O. Box 618, Boyers, PA, 16018-0618. Note: All forms must be signed within 120 days of the date of submission to

OPM. Submitted forms, which are not received within these 120 days, will be delayed or returned. If no change has occurred, forms must be re-dated and initialed by the Subject/employee.

If you require additional assistance for SF85P or related concerns, you may send email to SPAWARSYSCEN San Diego CA at SF85P@spawar.navy.mil.

Visit Authorization Letters (VALs) for Qualified Employees:

The contractor will include the IT Position Category for each person so designated on a VAL once the COR or TR has approved the Category. VALs will be sent to the following address: Commanding Officer, SPAWARSYSCEN San Diego, ATTN: Code 20352, 49275 Electron Drive, San Diego, CA 92152-5435.

Employment Terminations:

The contractor shall immediately notify the COR or TR, send email to SF85P@spawar.navy.mil, fax a termination VAL to Code 20352 at 619.553.6169, return any badge and decal to Code 20352, and replace any individual who has received a negative trustworthiness determination.

SPECIFIC ON-SITE SECURITY REQUIREMENTS

I. GENERAL.

a. Contractor Performance. In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD 254. The Contractor will conform to the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM). When visiting SPAWAR Systems Center at either the Point Loma Campus (PLC) or Old Town Campus (OTC) the Contractor will comply with the security directives used regarding the protection of classified and sensitive unclassified information, SECNAVINST 5510.36 (series), and SECNAVINST 5510.30 (series), and NRADINST 5720.1(series). A copy of these directives will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SPAWAR Systems Center's Security Contracting Officer's Representative (COR), Code 20351. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at SPAWAR Systems Center, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWAR Systems Center will exercise security supervision over all contractors visiting SPAWAR Systems Center and will provide security support to the Contractor as noted below. The Contractor will identify, in writing to Security's COR, an on-site Point of Contact to interface with Security's COR.

II. HANDLING CLASSIFIED MATERIAL OR INFORMATION.

a. Control and Safeguarding. Contractor personnel located at SPAWAR Systems Center are responsible for the control and safeguarding of all classified material in their possession. All contractor personnel will be briefed by their FSO on their individual responsibilities to safeguard classified material. In addition, all contractor personnel are invited to attend SPAWAR Systems Center conducted Security Briefings. In the event of possible or actual loss or compromise of classified material, the on-site Contractor will immediately report the incident to SPAWAR Systems Center's Code 20351 as well as the Contractor's FSO. A Code 20351 representative will investigate the circumstances, determine culpability where possible and report results of the inquiry to the FSO and the Cognizant Field Office of the DSS. On-site contractor personnel will promptly correct any deficient security conditions identified by a SPAWAR Systems Center Security representative.

b. Storage.

1. Classified material may be stored in containers authorized by SPAWAR Systems Center's PLC Physical Security Group, Code 20352 for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board SPAWAR Systems Center with Code 20352's written permission. Areas located within cleared contractor facilities on board SPAWAR Systems Center will be approved by DSS.

2. The use of Open Storage areas must be pre-approved in writing by Code 20352 for the open storage, or processing, of classified material prior to use of that area for open storage. Specific supplemental security controls for open storage areas, when required, will be provided by SPAWAR Systems Center, Code 20352.

c. Transmission of Classified Material.

1. All classified material transmitted by mail for use by long term visitors will be addressed to COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, 53560 HULL ST, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their code number.

2. All SECRET material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code 20332, for processing.

3. All CONFIDENTIAL material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Mail Distribution Center, Code 20331, for processing. This applies for either the OTC or PLC sites.

4. All SPAWAR Systems Center classified material transmitted by contractor personnel from the SPAWAR Systems Center will be sent via the SPAWAR Systems Center COR or TR for this contract.

5. The sole exception to the above are items categorized as a Data Deliverable. All contract Data Deliverables will be addressed to COMMANDING OFFICER, ATTN RECEIVING OFFICER CODE 223 SPAWAR SYSTEMS CENTER, 53560 HULL ST, SAN DIEGO, CA 92152-5410.

III. INFORMATION SYSTEMS (IS) Security. Contractors using ISs, networks or computer resources to process classified, sensitive unclassified and/or unclassified information will comply with the provisions of SECNAVINST 5239.3 (series) and local policies and procedures. Contractor personnel must ensure that systems they use at SPAWAR Systems Center have been granted a formal letter of approval to operate by contacting their Information System Security Officer (ISSO).

IV. VISITOR CONTROL PROCEDURES.

a. Contractor personnel assigned to SPAWAR Systems Center will be considered long-term visitors for the purpose of this contract.

b. Submission of valid Visit Authorization Letter (VAL) for classified access to SPAWAR Systems Center is the responsibility of the Contractor's Security Office. All VALs will be prepared in accordance with the NISPOM. They will be sent to either COMMANDING OFFICER, ATTN CODE 20352, SPAWAR SYSTEMS CENTER, 49275 ELECTRON DRIVE, SAN DIEGO, CA 92152-5435 for the PLC, or COMMANDING OFFICER, VISITOR CONTROL OTC, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO, CA 92152-5001 for OTC. Visit requests may be sent via facsimile to the PLC at (619) 553-6169, and verified on 553-3203 or the OTC at (619) 524-2745, and verified on 524-2751 or 524-3124. Visit requests may be submitted for a maximum of one year.

c. Visit requests for long-term visitors must be received at least one week prior to the expected arrival of the visitor to ensure necessary processing of the request.

d. Code 20352 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible SPAWAR Systems Center COR will request issuance of picture badges to contractor personnel. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of an SPAWAR Systems Center badge will be reported to the DSS. Identification badges must be worn in plain sight at all times on board SPAWAR Systems Center.

e. Prior to the termination of a Contractor employee with a SPAWAR Systems Center badge or active VAL on file the FSO must:

1. Notify in writing Code 20352, the COR, Security's COR, and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the termination and effective date. In emergency situations, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.

2. Confiscate any SPAWAR Systems Center identification badge and vehicle decal and return them to Code 20352 no later than 5 working days after the effective date of the termination.

V. INSPECTIONS. Code 20351 personnel will conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code 20351 representatives during these inspections. A

report of the inspection will be forwarded to the Contractor's employing facility and COR. The Contractor must be responsive to the Code 20351 representative's findings.

VI. REPORTS. As required by the NISPOM, Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication classified information has been lost or compromised. The Contractor will ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 20351. This reporting will include the following:

a. The denial, suspension or revocation of security clearance of any assigned personnel;

b. Any adverse information that would cast doubt on an assigned employee's continued suitability for continued access to classified information;

c. Any instance of loss or compromise, or suspected loss or compromise, of classified information;

d. Actual, probable or possible espionage, sabotage, or subversive information;

e. Any instance that would cast doubt on an assigned employee's trustworthiness to access Government ISs; or

f. Any other circumstances of a security nature that would effect the contractor's operation on board SPAWAR Systems Center.

VII. PHYSICAL SECURITY.

a. SPAWAR Systems Center will provide appropriate response to emergencies occurring onboard this command. The Contractor will comply with all emergency rules and procedures established for SPAWAR Systems Center.

b. A roving Contract Security Guard patrol will be accomplished by SPAWAR Systems Center. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to Code 20352.

c. All personnel aboard SPAWAR Systems Center are subject to random inspections of their vehicles, personal items and of them selves. Consent to these inspections is given when personnel accept either a badge or a vehicle pass/decal permitting entrance to this command.

VIII. COR RESPONSIBILITIES.

a. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions and/or submit a Final DD 254 to Security's COR.

b. Coordinates, in conjunction with the appropriate transportation element, a suitable method of shipment for classified material when required.

c. Certifies and approves Registration For Scientific and Technical Information Services requests (DD 1540) (DTIC).

d. Ensures that timely notice of contract award is given to host commands when contractor performance is required at other locations.

e. Certify need-to-know on visit requests and conference registration forms.

IX. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

Any cleared contractor facility on board SPAWAR Systems Center will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional SPAWAR Systems Center contracts may be authorized to use this cleared facility, but only on a case-by-case basis. The COR, Security's COR, and Contracting Officer must all be in agreement that this particular arrangement best suits the needs of the Government. At the end of this contract the on-site facility must be vacated, with proper written notification being submitted to the DSS and Security's COR.

X. ITEMS PROHIBITED ABOARD SPAWAR SYSTEMS CENTER.

a. Dangerous weapon, instrument or device includes, but is not limited to, the following:

rifles, automatic rifles, machine guns, sub-machine guns, pistols, machine pistols, flare pistols, starter pistols, shotguns, compressed gas, air or spring fired pellet or "BB" guns, sling shorts, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projective or other device which may injure someone;

daggers, switch blades, bow and arrows, sear guns, Hawaiian slings, power heads, fishing knives, scuba knives, or any unofficial knife with a blade longer than 2 1/2 inches;

martial arts devices (throwing stars, nunchakus), stun guns, tasers, brass knuckles, billy clubs, night sticks, pipe, bars, or mallets, or other similar devices capable of being used as a weapon;

poison, acids or caustic chemicals;

or any other item that may be used to inflict serious injury or death to another person or temporarily blind or disable an individual injury not specifically authorized by proper authority.

b. Explosive article or compound includes but is not limited to: ammunition for any of the small arms weapons mentioned as a dangerous weapon, including "blank" ammunition, gunpowder, Molotov cocktails, pipe bombs, grenades, pyrotechnics, fireworks or any other compound or article which might violently react and cause injury not specifically authorized by proper authority.

c. As an exception to the list of dangerous weapons, the possession of defensive tear gas devices (e.g., pepper spray) aboard all naval installations in California is now permissible. However, unauthorized use of these devices other than for self-defense will be prosecuted as a violation of the Uniform Code of Military Justice or applicable laws.

XI. ESCORTING POLICY.

a. All personnel within SPAWAR Systems Center's fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear an SPAWAR Systems Center issued badge. The word "Security" or "Safety" on selective Code 2035 or Code 2038 employee badges authorizes the bearer to escort unbadged emergency vehicles and operators and support personnel during emergencies. Only U.S. citizens and Permanent Residents may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SPAWAR SYSTEMS CENTER FOREIGN DISCLOSURE OFFICE, 20351.

b. All permanently badged SPAWAR Systems Center and tenant command employees, as well as those contractors and other government employees who have an "E" on their red and blue, respectively back grounded permanent badges may escort those visitors requiring an escort-required badge.

XIII. CONTRACTOR TRAINING.

All contractor personnel cleared Top Secret, Secret, or Confidential are required to receive annual Security Training. The issuance of a picture badge will trigger an e-mail to be sent to your personnel. This e-mail will give your employee the site of the computer-based training that must be completed. This training is required to be repeated annually.

FOR OFFICIAL USE ONLY (FOUO) INFORMATION

1. The For Official Use Only (FOUO) marking is assigned to information at the time of its creation. It isn't authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).

2. Use of FOUO markings doesn't mean that the information can't be released to the public, only that it must be reviewed by SPAWAR Systems Center San Diego CA prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

3. An UNCLASSIFIED document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the bottom face and interior pages.

4. Classified documents containing FOUO do not require any markings on the face of the document; however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY." Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion.

5. Any FOUO information released to you by SPAWAR Systems Center San Diego CA is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTION(S) _____ APPLY.

6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM SPAWAR SYSTEMS CENTER SAN DIEGO CA OR THE AUTHOR. When the FOUO status is terminated you will be notified.

7. You may disseminate FOUO information to your employees and subcontractors who have a need for the information in connection with this contract.

8. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items.

9. FOUO information may be transmitted via first-class mail, parcel post, fourth-class mail for bulk shipments only.

10. When no longer needed, FOUO information may be disposed by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash, or recycle, container or in the uncontrolled burn.

11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

12. Electronic transmission of FOUO information (voice, data, or facsimile) should be by approved secure communications systems whenever practical.